Envie d’un breuvage pressé ?

Une synthèse pour novices en intelligence artificielle:
Le procédé évoque le désir d’un artefact pour exécuter une action : afin de savourer un breuvage, il est nécessaire d’avoir une coupe. Si l’on ne possède pas de coupe, il faut en acquérir une. Pour cela, il faut au minimum un dollar. En l’absence de dollar, il est impératif de chercher un emploi. Si l’on se trouve dans l’incapacité de décrocher un emploi, il est essentiel de poursuivre des études. Si les ressources pour étudier font défaut, il est nécessaire de trouver un travail. En cas d’échec dans la quête d’un emploi, il est crucial de reprendre les études. Si l’on se retrouve coincé dans une boucle, il est vital d’obtenir un prêt. Pour accéder à un prêt, il faut disposer d’un bon historique de crédit. On peut aussi se satisfaire de boire du breuvage directement depuis le contenant.
Source : Narrabyte | Date : 2024-04-29 23:16:30 | Durée : 00:00:33

→ Accéder à CHAT GPT en cliquant dessus

Notification : Une lacune de sûreté capitale dans l’outil ConversationGPT pour Mac !

Lacune de sûreté dans l’outil ConversationGPT sur Mac

Lacune de sûreté dans l’outil ConversationGPT sur Mac

Les usagers de l’outil ConversationGPT sur Mac risquent de voir leurs informations exposées en raison d’une lacune de sûreté majeure.

ConversationGPT a la capacité d’analyser en temps réel le flux de votre caméra // Source : OpenAI

Une découverte toute récente met en lumière un souci sérieux de sûreté dans l’outil natif de ConversationGPT sur macOS. En effet, un programmeur a signalé que les données des usagers pourraient être exposées.

Un point faible inquiétant

Le programmeur Pedro José Pereira Vieito a partagé sur Mastodon les détails de cette lacune. D’après lui, l’outil

n’est pas sécurisé de manière appropriée, ce qui expose les informations des usagers à des risques éventuels.

Contrairement aux normes de sûreté habituelles, les demandes des usagers sont stockées dans un dossier non protégé, facilitant l’accès à ces données sensibles. Cette situation pourrait permettre à un programme malveillant d’espionner les discussions sans consentement.

Un risque pour la confidentialité des informations

Depuis MacOS Mojave (version 10.14), Apple a intensifié les mesures de protection des données personnelles des usagers. Cependant, la découverte de cette lacune dans l’outil ConversationGPT remet en question l’efficacité de ces mesures de sûreté.

En négligeant l’utilisation de la sandbox et en sauvegardant les conversations de manière non sécurisée, OpenAI compromet la confidentialité des informations des usagers. Cette lacune expose non seulement les échanges avec ConversationGPT, mais également d’autres informations sensibles en cas d’attaque.

Il est fortement recommandé d’attendre un correctif de la part de l’entreprise avant de télécharger ou de se servir de l’outil sur un appareil Mac. La sûreté des données personnelles doit demeurer une priorité absolue pour assurer une utilisation sûre et confidentielle de ConversationGPT.

Restez informés pour avoir plus de mises à jour concernant cette problématique de sûreté.